DETECTING PACKET DROPPING ATTACK IN WIRELESS AD HOC NETWORK

Sneha C.S[1] and Bonia Jose[2]

[1]Student, Department of Computer Science and Engineering, MBITS Nellimattom and
[2]Assistant Professor, Department of Computer Science and Engineering, MBITS Nellimattom

ABSTRACT

In wireless ad hoc network, packet loss is a serious issue. Either it is caused by link errors or by malicious packet dropping. The malicious nodes in a route can intentionally drop the packets during the transmission from source to destination. It is difficult to distinct the packet loss due to link errors and malicious dropping. Here is a mechanism which will detect the malicious packet dropping by using the correlation between packets. An auditing architecture based on homomorphic linear authenticator can be used to ensure the proof of reception of packets at each node. Also to ensure the forwarding of packets at each node, a reputation mechanism based on indirect reciprocity can be used.

KEYWORDS

Packet dropping, Homomorphic linear authenticator, Auditor, Indirect Reciprocity

1.INTRODUCTION

In a wireless ad hoc network, nodes communicate with each other via wireless links either directly or relying on other nodes as routers. The nodes in the network not only act as hosts but also as routers that route data to/from other nodes in network. An adversary may misbehave by agreeing to forward packets and then failing to do so. Once being included in a route, the adversary starts dropping packets. That means it stop forwarding the packet to the next node. The malicious node can exploit its knowledge about the protocol to perform an insider attack. It can analyze the importance of the transmitting packet and can selectively drop those packets. Thus it can completely control the performance of the network.

If the attacker continuously dropping packets, it can be detect and mitigate easily. Because even if the malicious node is unknown, one can use the randomized multi-path routing algorithms to circumvent the black holes generated by the attack. If the malicious nodes get identified, the node can be deleted from the routing table of network. The detection of selective packet dropping is highly difficult. Sometimes the dropping of packets may not be intentional. It can be occurred as a result of channel errors. So the detection mechanism should be capable of differentiating the malicious packet dropping and the dropping due to link errors.

The algorithm introduced here provides an efficient mechanism to detect the selective packet dropping. It improves the detection accuracy by calculating the correlation between lost packets with the help of Auto Correlation Function of the bitmaps at each node in the route. Bitmap describes the lost/received status of each packet in the transmission. The basic idea is that even

DOI: 10.5121/ijci.2016.5213

though malicious dropping may result in a packet loss rate that is comparable to normal channel losses, the correlation pattern is different.

To get the correct correlation, the truthfulness of the packet loss bitmaps is essential. In order to ensure the correctness the system uses a public auditing mechanism. The auditor uses a variation of the cryptographic primitive called homomorphic linear authenticator (HLA) [2].It is a signature scheme widely used in cloud computing and storage server systems, which allows client that has storeddata at an untrusted server to verify that the server possesses the original data without retrievingit [3]. Indirect reciprocity is a powerful mechanism for the evolution of cooperation between nodes. The essential concept of indirect reciprocity is "I help you not because you have helped me but because you have helped others" [12].

The remainder of this paper is organized as follows. In Section 2 we review the related work. The system models and problem statement are described in Section3. We present the proposed mechanism in Section 4 and we conclude the paper in Section 5.

2.RELATED WORKS

Based on how much weight a detection algorithm gives to link errors relative to malicious packet drops, the works had been done to detect the malicious packet dropping can be broadly classified into two.

First category focuses on the detection with high malicious dropping rates, where the link errors are ignored. Based on the nature of the detection algorithm, this can be further classified into four. The first sub-category is based on credit systems [9].In this node gets incentive for its cooperation in transmission. When the node correctly transmits the packets to the next hop, it gets credit. Based on the credit value, the node gets priority during the transmission of its own packets. Thus, when the attacker continuously drops packets, its credit decreases and automatically gets expelled from the network. But when the attacker performs a selective dropping, it gets enough credits and can continue as a part of the network. The second sub category is based on reputation systems [4], [5], [6], [7]. In this mechanism the neighbour nodes monitor the activity of all nodes. For a node that drops packets maliciously gets a bad reputation. The reputation is the determining factor while selecting a route for transmission. Thus malicious nodes get excluded from a route. In this mechanism also, if the attacker selectively drop packets and forward some packets, then it can have a better reputation. The third sub category of works focus on the hop to hop acknowledgement, by which it can directly find out the misbehaving node. The fourth sub category uses cryptographic methods for the detection purpose. For example, the work in [8] utilizes Bloom filters to construct proofs for the forwarding of packets at each node. By examining the relayed packets at successive hops along a route, one can identify suspicious hops that exhibit high packet loss rates. But the incorrect proofs will reduce the detection accuracy of this mechanism.

The second category of works focus on the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible. This type of mechanisms requires the knowledge of the wireless channel. The works in [9] and [10] proposed to detect malicious packet dropping by counting the number of lost packets. If the number of lost packets is significantly larger than the expected packet loss rate made by link errors, then with high probability a malicious node is contributing to packet losses. But counting the number of lost packets is not sufficient to detect the attacker. That is, if the

attacker selectively drop packet then the count of lost packet due to malicious node and the link may get equal.

All methods mentioned above do not perform well when malicious packet dropping is highly selective. But the detection of packet dropping using the correlation between lost packets gives better solution for selective packet dropping.

The methods in [14] delay a jammer from recognizing the significance of a packet after the packet has been successfully transmitted, so that there is no time for the jammer to conduct jamming based on the content/importance of the packet. Instead of trying to detect any malicious behavior, the approach in [14] is proactive, and hence incurs overheads regardless of the presence or absence of attackers.

3.SYSTEM MODEL AND PROBLEM STATEMENT

3.1.System Model

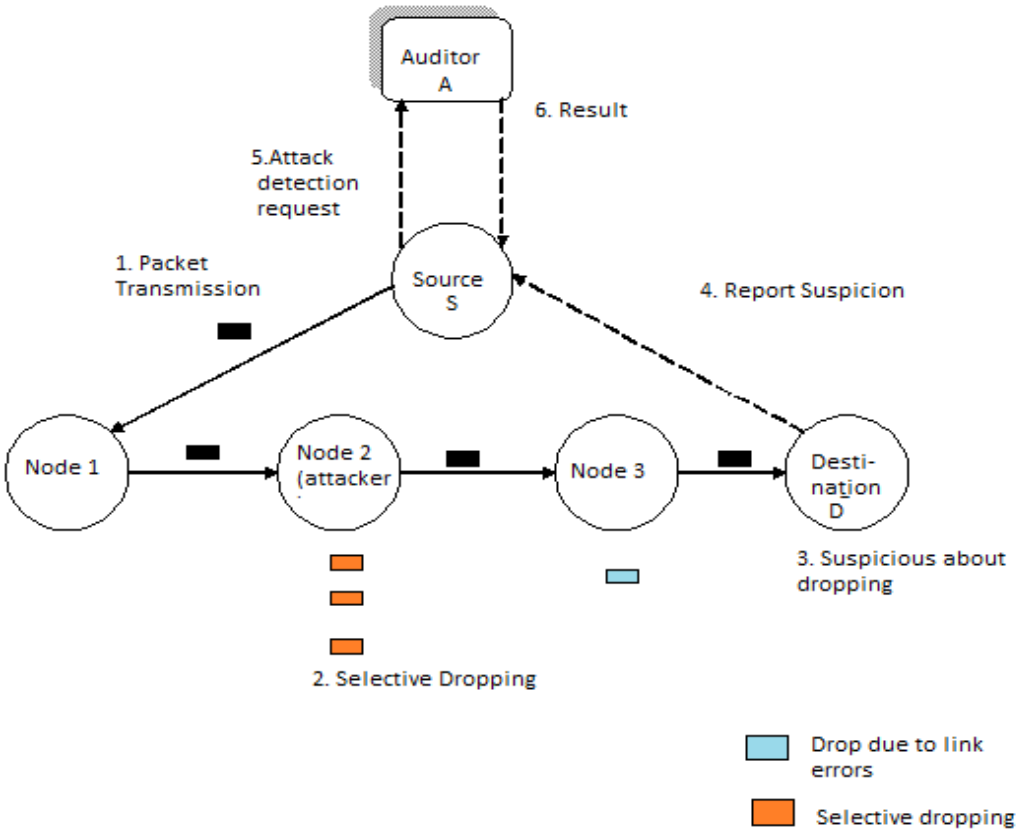

Figure1. System Model

Let P_{SD} be an arbitrary route in a wireless ad hoc network. The source S is aware of the path and it sends packets continuously to the destination D through P_{SD}. Consider that the network is quasi-static type. That means the network topology and link characteristics are constant for a relatively long period of time. Each hop that constitutes the path alternates between good and bad states. Packets transmitted during the good state are successful, and packets transmitted during the bad state are lost. By observing whether the transmissions are successful or not, the receiver obtains a realization of the channel state, which is a combination of zeros and ones. In that "1" denotes the packet was successfully received, and "0" denotes the packet was dropped.

When the receiver notifies some suspicious packet loss, it reports a feedback to the sender. The detection of malicious dropping is performed by an independent auditor module. After receiving the feedback from the receiver, sender requests the auditor to perform detection. The auditor module identifies the malicious dropping by checking the correlation between lost packets at each node. The correlation between lost packet in selective dropping condition and link error condition is different [1]. For this, the information collected by the auditor will be accurate. In order to ensure that the packet received by a node, the mechanism proposed here uses a homomorphic linear authenticator. Also, to ensure the packet forwarding, it uses a reputation based mechanism which uses an indirect reciprocity framework based on evolutionary game theory, described in [11].

3.2.Problem Statement

The adversary, which is a node in the path, may try to degrade the performance of the system by dropping the packets send by the source. The node can perform the dropping selectively or randomly. The detection should be done by an independent auditor module. While performing detection it should verify the correctness of collected information. Also, should produce a publically verifiable proof of the misbehaviour of the node.

Besides this there is a chance for collusion between two nodes. A covert communication channel may exist between any two malicious nodes, in addition to the path connecting them on PSD. As a result, malicious nodes can exchange any information without being detected by Ad or any other nodes in PSD. Malicious nodes can take advantage of this covert channel to hide their misbehavior and reduce the chance of being detected.

4.DETECTION OF PACKET DROPPING

4.1.Overview

The detection mechanism focuses on the correlation between the lost packets at every node in the transmission route. While the sender S transmitting the packets consecutively, each hop in the path will keep a transmission bitmap for every packets. The bitmap is a pattern of 0 and 1, where 1 represents the successfully transmitted packet and 0 represents the unsuccessfully transmitted packets. By using an Auto Correlation Function (ACF), the correlation between these bitmaps can be calculated. Under different packet dropping conditions the correlation function will generate different values. Thus by observing the correlations between lost packets, one can decide whether the packet loss is purely due to regular link errors, or is a combined effect of link error and malicious drop.

But the main challenge is that the packet-loss bitmaps reported by individual nodes along the route may not be correct. For the correct calculation of the correlation between lost packets the truthfulness of bitmap is necessary. This can be achieved by auditing functionality. Auditing can be done by using a cryptographic primitive called homomorphic linear authenticator (HLA), which is a signature scheme to provide a proof of storage from the server to entrusting clients in cloud computing and storage server systems. Besides this to ensure the forwarding, a reputation based mechanism can be used. When a node relays packet successfully, it gets a good reputation from the receiving node. That means, in a path from sender to receiver, the node with minimum reputation dropped more packets.

4.2.System Architecture

In a wireless ad hoc network, the source S is supposed to send the packets to the destination D continuously, through the wireless channel P_{SD}. Here we are considering the quasi-static networks. So the path P_{SD} remains unchanged for a long time. While receiving a sequence of packet, the receiver gets a realization of channel state simply by observing whether the transmissions are successful or not. Successfully received packets are denoted by 1s and others are denoted by 0s. Each node in P_{SD} will also provide a reputation to the relying node when it gets a packet.

There is an auditor A_d in the network. It is not associated with any node and kept as independent. It is totally unaware of the secrets shared between nodes in the path P_{SD}. The detection of malicious packet dropping is performed by this auditor. When the receiver finds out some abnormality in the reception of packets, it will report the suspicion to the source. Once being notified the source send submits an attack-detection request (ADR) to the Auditor.

For the detection of attack, the auditor will collect the information about transmission from each node on the path P_{SD}. The auditor needs to verify authenticity of the collected information. Once the truthful information is collected from every node in the route, the auditor calculates the correlation between them. From this information, it can detect the attack.

4.3.Scheme Details

The system consists of four Phases:

i. Setup Phase

ii. Packet Transmission Phase

iii. Audit Phase

iv. Detection Phase

4.3.1.Setup Phase

Immediately after establishing the route, the setup phase gets started. The source decides on symmetric key crypto system for encryption the packet during the transmission phase. Source securely distributes a decryption key and a symmetric key to each node on the path. Key distribution may be based on the public-key crypto-system. The source also announces two hash functions to every node in the route. Besides this, source also needs to set up its HLA keys.

4.3.2.Packet Transmission Phase

After the successful completion of Setup phase, source enters into the transmission phase. In this phase, before the transmission of packets source computes the hash value of each packet and generates HLA signatures of the hash value for each node. These signatures are then sent together with the packets to the route by using a one-way chained encryption. This prevents the deciphering of the signatures for downstream nodes by the upstream node. When a node in the route receives the packet from source it extracts packets and signature. Then it verifies the integrity of received packet. A database is maintained at every node on P_{SD}. It can be considered as a FIFO queue which records the reception status for the packets sent by source. Every node stores the received hash value and signature in the database as a proof of reception.

To ensure the relying at each node an indirect reciprocity framework based on evolutionary game theory can be used. In this method each node is considered as a player. Generally, helping someone establishes a good reputation, and will be rewarded by others. In this paper, we adopt the reputation updating rule of indirect reciprocity in [12], i.e., the reputation of relay is updated according to the following rule:

	G	B
F	G	G
D	B	G

where a relay who takes the choice X($X \in \{F,D\}$) towards a provider with reputation R ($R \in \{G,B\}$) will be assigned a new reputation R(R;X) ($R \in \{G,B\}$). Here, we adopt the reputation updating such that cooperation leads to a good reputation, whereas defection leads to a bad reputation unless the opponent is a bad player. The total value of reputation can be calculated by subtracting bad reputation from good.Nodes will also keep another database to keep the reputation value.

4.3.3.Audit Phase

When the source issues an attack detection request (ADR), the audit phase gets started. The ADR message includes the id of the nodes on the route, source' s HLA public key information, the sequence numbers of the packets sent by source, and the sequence numbers packets that were received by destination . The auditor requests the packet bitmap information from each node in the route by issuing a challenge. From the information stored on the database, every node generates this bitmap. Auditor checks the validity of bitmaps and accepts if it is valid. Otherwise it rejects the bitmap and considers the node as a malicious one.

This mechanism only guarantees that anode cannot understate its packet loss, i.e., it cannot claim the reception of a packet that it actually did not receive. This mechanism cannot prevent a node from overly stating its packet loss by claiming that it did not receive a packet that it actually received. This latter case is prevented by the mechanism based on reputation which is discussed in the detection phase

4.3.4.Detection Phase

After auditing the reply to the challenge issued by the auditor, it enters into the detection phase. Auditor constructs per hop bitmaps and by using an auto correlation function (ACF) it will find out the correlation between the lost packets. Then it finds out the difference between the calculated value and correlation value of wireless channel. Based on the relative difference, it decides whether the packet loss is due to the malicious node or link error. When it finds out malicious drop, it can consider both ends of the hop as suspicious. That means either the transmitter did not send the packet or receiver did not receive.

After identifying these two suspicious nodes, the detector needs to find out the actual culprit. For this, it can check the reputation value. Now the Auditor module will collect the reputation value for the two suspicious nodes. When a node fails to forward the packet it, it will get minimum reputation. By checking this, the detector can easily distinguish the attacker.

5.CONCLUSIONS

In order to detect the malicious node that drops the packets intentionally, the technique described here utilizes the correlation between the lost packets at each node in the route from source to destination. . For this, uses a public auditing architecture. This mechanism will give a satisfactory improvement in the detection accuracy of selective packet dropping. To correctly calculate the correlation between lost packets, it requires truthful packet loss information from every node in the route. Auditor ensures the integrity of packet loss information of each individual node by using Homomorphic Linear Authenticator (HLA). HLA-based public auditing architecture ensures truthful packet-loss reporting by individual nodes. This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route.

Based on the indirect reciprocity mechanism, we have theoretically analyzed the evolutionary dynamics of cooperative strategies. The reputation mechanism will ensure the correct forwarding process. Due to the evolutionarily stable strategies based on indirect reciprocity is effective and robust against packet loss and imperfect estimation of reputation.

REFERENCES

[1] Tao Shu, Marwan Krunz, "Privacy – Preserving and Truthfull Detection of Packet Dropping Attacks in Wireless Ad Hoc Networks",April 2015.

[2] C. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proc. ACM Conf. Comput. andCommun. Secur., Oct. 2007,pp. 598–610.

[3] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in Proc. IEEE INFOCOM Conf., Mar. 2010, pp. 1–9

[4] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H.Rubens, "ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inform. Syst. Security, vol. 10, no. 4, pp. 1–35, 2008.

[5] S. Buchegger and J. Y. L. Boudec, "Performance analysis of the confidant protocol (cooperation of nodes: Fairness in dynamic adhoc networks)," in Proc. 3rd ACM Int. Symp. Mobile Ad Hoc Netw.Comput. Conf., 2002, pp. 226–236.

[6] W. Galuba, P. Papadimitratos, M. Poturalski, K. Aberer, Z. Despotovic, and W. Kellerer, "Castor: Scalable secure routing for ad hoc networks," in Proc. IEEE INFOCOM, Mar. 2010, pp. 1 –9.

[7] Q. He, D. Wu, and P. Khosla, "Sori: A secure and objective reputation-based incentive scheme for ad hoc networks," in Proc. IEEE Wireless Commun. Netw. Conf., 2004, pp. 825–830.

[8] W. Kozma Jr., and L. Lazos, "REAct: Resource-efficient accountability for node misbehavior in ad hoc networks based on random audits," in Proc. ACM Conf. Wireless Netw. Secur., 2009, pp. 103–110.
[9] T. Hayajneh, P. Krishnamurthy, D. Tipper, and T. Kim, "Detecting malicious packet dropping in the presence of collisions and channel errors in wireless ad hoc networks," in Proc. IEEE Int. Conf. Commun., 2009, pp. 1062–1067.
[10] S. Zhong, J. Chen, and Y. R. Yang, "Sprite: A simple cheat-proof,credit-based system for mobile ad-hoc networks," in Proc. IEEE INFOCOM Conf., 2003, pp. 1987–1997.
[11] Changbing Tang, Ang Li, and Xiang Li, "When reputation enforces evolutionary cooperation in unreliable MANETs", Nov. 2014
[12] M. A. Nowak, and K. Sigmund, "Evolution of indirect reciprocity," *Nature*, vol. 437, pp. 1291 1298, Oct. 2005.
[13] H. Ohtsuki, Y. Iwasa, and M. A. Nowak, "Indirect reciprocity provides only a narrow margin of efficiency for costly punishment," *Nature*, vol.457, pp. 79-82, Jan. 2009.
[14] A. Proano and L. Lazos, "Selective jamming attacks in wireless networks," in Proc. IEEE ICC Conf., 2010, pp. 1–6.

AUTHORS

Sneha C.S currently pursuing M.Tech in Computer Science and Engineering in MBITS Nellimattom. She received B.Tech in Computer Science and Engineering from MBITS, Nellimat tom, M.G University, Kottayam,India in 2013. Her area of interest includes cyber security.

Bonia Jose received **B.Tech**Degree in Computer Science and Engineering from Viswajyothy College of Engineering and Technology, Vazhakkulam and **M.Tech** fromKarunya University, C oimbatore. She is currently working as Assistant professor at MBITS Nellimattom. She is specialized in Networking and Internet Engineering.